UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF WISCONSIN

In the Matter of the Search of

Premises located at 623 W. Lincoln Ave., Oshkosh, WI, further described as a two story multi-family residence, beige in color with wood siding, white trim and dark green shingled roof.

APPLICATION & AFFIDAVIT FOR SEARCH WARRANT

Case Number: 05-M622

I, ROBERTO MOLINA, being first duly sworn depose and state:

I am a Special Agent with the Federal Bureau of Investigation, and have reason to believe that on the property or premises known as:

Premises located at 623 W. Lincoln Ave., Oshkosh, WI, further described as a two story multi-family residence, beige in color with wood siding, white trim and dark green shingled roof. There are separate entrances with separate street addresses for each of the residences that make up this multi-family dwelling. The front door to the residence has the number "623" written above it. There is also a rear door to the residence with the number "623" written above it.

in the Eastern District of Wisconsin there is now concealed certain property, namely: See Attachment B

which is: **evidence of the commission of crimes, contraband, or other items illegally possessed,** concerning violations of Title 18, United States Code, § 2252.

The facts to support a finding of Probable Cause are as follows: **Please see attached affidavit of FBI SA Roberto Molina incorporated by reference herein.**

Continued on the attached sheet and made a part hereof. ✓ Yes / No

Signature of Affiant: Roberto Molina

Sworn to before me, and subscribed in my presence

May 25, 2005; 4:45 PM
Date and time issued

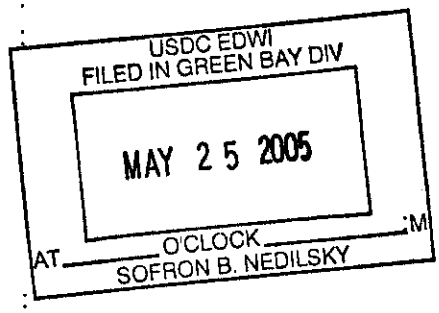
at Green Bay, Wisconsin
City and State

HONORABLE WILLIAM C. GRIESBACH
United States District Judge
Name & Title of Judicial Officer

Signature of Judicial Officer

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN

IN THE MATTER OF THE
SEARCH OF
Premises located at 623 W. Lincoln Ave., Oshkosh, WI more particularly described as a two story multi-family residence, beige in color with wood siding, white trim and dark green shingled roof.



Case No. 05-M 622

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Robert Molina, being duly sworn, depose and state:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), assigned to the Green Bay, Wisconsin Field Office/Resident Agency. I have been so employed for approximately fourteen years. As part of my daily duties as an FBI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A.[1] I have received training in the area of child pornography and child exploitation, including a course at the National Advocacy Center, Columbia, South Carolina entitled Investigation and Prosecution of Advanced Child Exploitation Cases, and I have had the opportunity to observe and

[1] The language "visual depictions involving the use of a minor engaging in sexually explicit conduct" as used in 18 U.S.C. §2252(a) is also being referred to in this document as "child pornography."

review numerous examples of child pornography (as defined in 18 U.S.C. § 2256)[2] in all forms of media including computer media. I have also participated in the execution of approximately thirty search warrants, of which approximately ten search warrants have involved child exploitation and/or child pornography offenses.

2. This Affidavit is made in support of an application for a warrant to search the entire premises located at 623 W. Lincoln Ave., Oshkosh, WI (the "SUBJECT PREMISES"). The SUBJECT PREMISES to be searched is more particularly described as follows based on my personal observation of it: a two story multi-family residence, beige in color with wood siding, white trim and dark green shingled roof. There are separate entrances with separate street addresses for each of the residences that make up this multi-family dwelling. There is a door with the number "623" written above it that I would consider the front door for that residence. There is also a door to the rear of the residence with the number "623" written above it that I believe to be a second entrance into the residence.

3. The purpose of this application is to seize evidence of violations of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess child pornography, and violations of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2), which make it a crime to

---

[2] "Child Pornography means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; . . . [or] (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct." For conduct occurring after April 30, 2003, the definition also includes "(B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaging in sexually explicit conduct." 18 U.S.C. § 2256(8).

distribute and receive child pornography in interstate commerce by computer, and §§ 2252(a)(1) and 2252A(a)(1), which make it a crime to transport or ship child pornography in interstate commerce.

4. I am familiar with the information contained in this Affidavit based upon the investigation I have personally conducted and based on my conversations with other law enforcement officers involved in this investigation.

5. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252 and 2252A are located at the SUBJECT PREMISES including within a computer and related peripherals, and computer media found at the SUBJECT PREMISES. Where statements of others are set forth in this Affidavit, they are set forth in substance and in part.

6. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§ 2252 and 2252A, are present at the SUBJECT PREMISES.

7. The instant investigation has revealed that an individual assigned the Internet Protocol address ("IP address") 69.23.82.99 at 14:06 CST on March 8, 2005, subsequently identified as being associated with Samantha Vollmer possessed child pornography on a computer that is located at the SUBJECT PREMISES and received child pornography from another computer user. Paragraphs 8 through 19 explain computer-related technical terms and concepts relevant to this investigation. Paragraphs 20 and 21 explain how

computers and computer technology have revolutionized the way in which child pornography is produced, utilized and distributed. The information set forth in paragraphs 22 through 34 provide background concerning the underlying investigation undertaken through which the lead to the SUBJECT PREMISES was developed. Finally, paragraphs 35 through 41 describe, more particularly, the investigation of the SUBJECT PREMISES.

The Internet and Definitions of Technical Terms Pertaining to Computers and F-Serves

8. As part of my training, I have become familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers[3] and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via electronic mail ("e-mail"). An individual who wants to use the Internet may do so at public locations such as Internet

[3] **Computer**: The term "computer" is defined by 18 U.S.C. § 1030(e)(1) to mean "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

cafes or the public library or they may contract privately by obtaining an account using a personal computer that is linked to the Internet – for example, through a university, an employer, or a commercial service – which is called an "Internet Service Provider" or "ISP" (see definition of "Internet Service Provider" below).

9. The Internet and the World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

10. Collectors and distributors of child pornography can also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as America Online (AOL), Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

11. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as in temporary files or ISP client software,

among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence indicating whether a computer contains file serving or peer-to- peer software, for example, when the computer was sharing files, and files that have been uploaded or downloaded. Such information is often maintained for very long periods of time until overwritten by other data.

12. A computerized depiction of child pornography is often stored and referred to as a GIF, short for Graphic Interchange Format, or a JPEG, short for Joint Photographic Experts Group. These image files often contain images or photographs that have been converted into a computer format by the use of a scanner or were originally taken in a digital format. A single image may be recorded as a single computer file. However, a file may contain two or more images (sometimes more than 100), and these files are often referred to as ZIP files, referring to their compressed archive format. Another type of file is called an MPEG, short for Moving Picture Experts Group. An MPEG is a file containing a movie or video clip.

13. Through my experiences and training as a Special Agent in the Innocent Images National Initiative, I know the following to be true:

14. Internet Relay Chat (IRC) is a method of communication available to Internet users through the use of special software. The communication between users is made possible by a network of computers known as servers. The special IRC software, known as an IRC client, acts as the means to access the IRC servers. The software

accepts data, usually text, from the user and sends it to the IRC server(s). The data is then distributed by the server(s) and received by the IRC client in use by another user. The sender of the data can select whether the message is viewed by all users currently online or by only certain users. Thus, it is possible to 'chat' in a public forum, or, more privately, user to user.

15. Another function available to IRC users is the ability to create a direct client to client (DCC) connection between two users. One of the ways to establish a DCC connection is through use of a special software program known as a File Transfer Protocol or FTP program. Once established, this type of connection allows one user (the guest) to directly access a portion of the other user's (the host's) hard disk or other storage medium. The host computer is known as a "**file server**" or "**F-Serve**" because it is set up to serve files to other users. In order to access an F-serve, the guest user must enter a password (known as a "trigger") that the host typically has posted on the IRC channel. Once the guest types in the password, he can access the host's computer (now a file server) and send (upload) or receive files from the host's computer. Once the transfer is completed, the direct connection is terminated and the users may resume 'chatting' as before. The files obtained may be items such as written documents or graphic images which have been scanned and recorded in computer format, or otherwise exist in a digital format.

16. The exchange of images using the above method is common among collectors of child pornography. In order to build a larger collection, a collector will usually grant a guest a certain amount of credit to download images from the collector's F-Serve.

Once exhausted, the guest must transmit (upload) an image to obtain more credit to receive (download) additional images. Often, the operator of the F-Serve will establish a ratio which determines the amount of credit, measured in bytes, that the user will receive for each image that is uploaded. For example, if a ratio of 1 to 5 is set by the operator of the F-Serve, the guest will receive 5 bytes of credit for each byte uploaded.

17. There are many different IRC networks. That is, there are many groups of IRC servers. Each group of servers is called a network and has a name such as "Undernet," "DalNet" or "EuNet". On each network, there are many (often up to several thousand) channels. Each channel is assigned a name which generally refers to the topic of conversation or interest in that channel. A user may log on to one or more channels and participate in the online conversation(s) or simply observe. Once in a channel, if both users concur, a DCC connection can be established for the exchange of computer files.

18. A user of an IRC network is identified to other users by only a nickname which he or she selects. This name, known as a 'nick', may be any unique combination of characters and may be changed at any time. Because the user may enter anything as a 'nick,' IRC is a fairly anonymous form of communication. Also, aside from the system operators who ensure the proper operation of the servers, there is no regulating authority in control of this communication medium. The only identifying data over which the user has no control is his or her Internet Protocol (IP) address. This address, expressed as a four numbers separated by decimal points, is unique to a particular computer during an online sessions.

19. Set forth below are some definitions of technical terms, used throughout this Affidavit, and in Attachments A and B hereto, pertaining to the Internet and computers more generally.

a. **Computer system and related peripherals, and computer media**: As used in this affidavit, the terms "computer system and related peripherals, and computer media" refer to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, CDs, DVDs, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation equipment, digital cameras, compact flash cards, scanners, in addition to computer photographs, Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats, including, but not limited to, JPG, GIF, TIF, AVI, and MPEG.

b. **Internet Service Providers (ISPs) and the Storage of ISP Records**: Internet Service Providers are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription.

ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("ISP records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files. Typically, e-mail that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "electronic storage," see 18 U.S.C. § 2510(17), and the provider of such a service is an "electronic communications service. " An

"electronic communications service," as defined by statute, is "any service which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is defined by statute as providing a "remote computing service." 18 U.S.C. § 2711(2).

c. **IP Address**: Every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 254. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing, that is they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial-up modem will be assigned an IP address from a pool of IP addresses for the duration of each

dial-up session. Once the session ends, the IP address is available for the next dial-up customer. On the other hand, some ISP's, including most cable providers, employ static IP addressing. In that instance, a customer or subscriber's computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. In other words, a static IP address is an IP address that does not change over a period of time and is typically assigned to a specific computer.

Computers and Child Pornography

20. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, individuals who

distribute child pornography over the Internet use different tools, such as file server software, P2P file sharing software, etc. to conduct the transfer of the content, allowing them to remain relatively anonymous.

21. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, the development of computers has also revolutionized the way in which child pornography collectors interact with, and sexually exploit, children. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by child pornography collectors in these ways:

a. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce,

store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

b. The Internet allows any computer to connect to another computer. Electronic contact can be made to literally millions of computers around the world.

c. The Internet allows users, while still maintaining anonymity, to easily locate (I) other individuals with similar interests in child pornography; and (ii) websites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet.

d. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard

drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 80 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

Background of the Underlying Investigation

22. On January 11, 2005, FBI SA Matthew Zentz, while acting in an undercover capacity, logged on to Internet Relay Chat (IRC) for purposes of locating individuals distributing child pornography via IRC F-serves. SA Zentz entered the chat channel "#100%preteenboysexpix" and observed an individual with the nickname "Ownage69" who was advertising an F-serve with the password, or trigger command, "!BoysRcute." SA Zentz also observed that "Ownage69" had set up a ratio of 1:1, that is, one picture or movie file could be downloaded for every picture or movie file uploaded. Further, SA Zentz observed the following rules set up by "Ownage69" as part of his advertisement: "If you are with or work for any of the following: Police, FBI, Undercover, Reporter or trying to gather information about my site you MUST LEAVE NOW!!!!!". You MUST send PICTURES ONLY, The picture MUST have a boy under the age of 12 years old or

hairless. I am NO LONGER ACCEPTING clothed boys unless the series has nude boys in it, you MUST send the NUDE picture first. NO WEB SITE PICS, NO RENAMES, NO MOVIES are allowed!!! Only accepting NEW SERIES and PICS at this time, If I stop your file it means I have the series or pic."

23. SA Zertz entered the F-server of "Ownage69" that day and viewed the directory he made available. Within the "Ownage69" directory, SA Zertz observed folders under the headings "GIRLPICS", "OTHERBOYSPICS", "TEENBOYPICS", AND "WHITEBOYSPICS". SA Zertz reviewed the file names available within "GIRLPICS" and observed several sub directories named "GIRLS UNSORTED ON CD", "NOTONCD", and "SERIES". Within the directory "GIRLPICS", approximately 600 files, all believed to be image files given the "jpg" extension, were found. Many of the files had names suggestive of child pornography, such as "!!!!9yrldfuckedhard.jpg" and "(porn) children-very young girl raped by dog.jpg".

24. Within the folder "OTHERBOYSPICS", SA Zertz found another folder entitled "UNDER5" which included a series entitled "DIAPERS". Within this folder approximately 50 files, believed to be image files, were located. Some of these files had names suggestive of child pornography, such as "02yrdiapercum08.jpg". Within the folder "WHITEBOYSPICS", SA Zertz observed in excess of twenty other sub directories with titles such as "SPANK", "MESSY", "BOY_GIRL_PICS", "PISS", "UNSORTED NOT ON CD" and "UNDER_5".

25. From "Ownage69"'s F-serve folder "WHITEBOYSPICS", SA Zentz downloaded 80 image files including: "babyboy&dadanal4.jpg"; "babyboy.jpg"; "boy_rapes_baby.jpg";

"why_men_have_two_hands.jpg"; "baby_cumface_01.jpg"; "baby_cumface_02.jpg";"boyrape2.jpg"; "6yofuckdaddy.jpg"; babytorture157107551g.jpg"; and "mom_licks_baby.jpg". Many depicted infants and young children engaging in sexually explicit conduct. For example, the following is the name of the image file downloaded and a brief description of the image: "baby_cumface_01jpg" (depicts an adult male ejaculating on a baby's head); "babydad2.jpg" (infant holding adult males erect penis); and "baby_cumface_03.jpg" (adult male placing erect penis into baby's mouth). SA Zentz uploaded encrypted images to satisfy the requirement that he upload files in order to download files.

26. On March 16, 2005, the FBI executed a search warrant at the residence of Keith Reimann, located at 1221 Parrot Street, Green Bay, Wisconsin. Mr. Reimann was home at the time. A search of the bedroom occupied by Mr. Reimann resulted in the recovery of a computer with multiple hard drives, numerous media storage devices including compact disks and DVD's, and a digital camera. Mr. Reimann was subsequently interviewed and admitted that he was responsible for operating an F-serve. He further stated that he had been operating the F-serve only within two channels on IRC entitled "#100%preteenboysexpix" and "#100%preteenboysexpics."

27. A forensic computer examination was conducted by Lam Nguyen, of the High Technology Investigative Unit at the Department of Justice on the multiple computer hard drives recovered from Mr. Reimann's bedroom. The examination confirmed the presence of F-serve software operating within the two IRC chat channels "#100%preteenboysexpix" and "#100%preteenboysexpics." The F-serve contained the

same advertisement and rules observed earlier in the IRC channel visited by SA Zentz. Mr. Nguyen identified in excess of 150,000 image files available for downloading from Mr. Reimann's F-serve most of which were sorted by content and placed in folders that accurately summarized the image content. Mr. Nguyen's analysis further showed that since approximately January, 2005, in excess of 4,700 files were uploaded to Mr. Reimann's F-serve and on approximately 10,020 occasions, Mr. Reimann distributed movie and image files to individuals who accessed his F-serve.

28. During the forensic examination of Mr. Reimann's computer, Mr. Nguyen discovered that Mr. Reimann was utilizing Panzer File Server software, a specific type of file server software used on the IRC.

29. Panzer File Server software maintains log records of every person (hereinafter a "client") who logs in and out of a particular server. These records are kept automatically, in part to keep track of when a particular client logged in and out of the server, and how many credits a particular client has left. (see paragraph #16 above regarding the use of "credits" in a file sharing server).

30. Each particular log file created by the File Panzer Server is identified by a combination of the client's user name and IP address. In other words, each client who logs onto the file server has a log automatically created about him/her by the software, in order to track that client, and that log is identified by the client's username and IP address. These log files are called INI files.

31. Each INI file contains information about a client. Specifically, it contains the creation date and time that the log file is first created (which corresponds to the date and time the

client first accesses the file server), the last date that the client visited the file server, all files uploaded and/or downloaded by the client, and where the uploaded or downloaded files were stored or where they came from.

32. In his examination of Mr. Reimann's computer, Mr. Nguyen was able to recover over 500 INI files, with creation dates between January and March of 2005. Mr. Nguyen then conducted an investigation to determine which INI files related to individuals with IP addresses within the United States.

33. The Child Exploitation and Obscenity Section of the United States Department of Justice, and the United States Attorney's office for the Eastern District of Wisconsin, sent legal process to the ISP for each IP address identified as a domestic IP address, in order to determine the user associated with that IP address at the specific date and time identified by the INI file stored on Reimann's computer.

34. One of the responses received showed that the IP address 69.23.82.99 utilized on March 8, 2005 was subscribed to by Samantha Vollmer, 623 W. Lincoln Ave. Oshkosh, WI 54901.

Probable Cause to Search the Subject Premises

35. In addition to my own investigation, I have also reviewed materials prepared and sent to me by Mr. Nguyen which includes the materials collected about the target during the initial investigation. Among those materials were the user's IP address, which was 69.23.82, the original INI file for that IP address showing the time the user had been online, which was March 8, 2005 at 14:06 CST, the User's ISP, which is Time Warner-Road Runner, the files posted/received during that on line session, and the users on line

nickname "Jennybif@69.23.82.99.".

36. The subpoena return from Time Warner- Road Runner showed that the user with IP address 69.23.82.99 who was online at 14:06 on March 8, 2005 was a customer of the ISP identified as Sandra Vollmer whose billing address is 623 W. Lincoln Ave. Oshkosh, WI 54901 and with telephone number (920) 213-0294 - the SUBJECT PREMISES.

37. Time Warner-Road Runner also confirmed that Vollmer's account is still active. According to the ISP, Vollmer gave a day phone number of (920) 213-0294 and has a username "svollmer1."

38. I have also been able to view the images identified through the forensic computer examination conducted by Mr. Nguyen as having been downloaded from Reimann's F-Serve by the user of the IP address 69.23.82.99 at 14:06 CST on March 8, 2005. Those images include the following: (1) nine different images of a post-pubescent, naked minor, several images of which showed the lascivious exhibition of his genitals; (2) one image of a prepubescent girl with legs spread and an adult hand spreading her vaginal area; (3) one image of a prepubescent female, naked with legs spread and vagina area exposed; and (4) five images of an adult male and prepubescent girl, both individuals are naked, and one image of which shows the girl straddling the adult males chest while the adult male is touching his penis. I believe most of these images constitute child pornography. The images uploaded by the individual associated with IP address 69.23.82.99 include approximately 15 images none of which constitute child pornography but some of which are sexually explicit images of individuals between the ages of 18 and 25.

39. On May 24, 2005 in the early afternoon, I had an employee of FBI call the telephone

number of (920) 213-0294 and use the ruse that she was calling about customer satisfaction with Road Runners internet service. A female subject answered the telephone and stated that her name was Samantha. Samantha confirmed that her address was 623 W. Lincoln Ave., Oshkosh, WI 54901. Samantha further advised that she and her other two roommates all used the computer for internet connections. She further advised that the internet access was for her residence and not for a business. She further advised that there was no wireless service associated with her computer.

40. Postal authorities verified through the United States Postal Service database that Samantha Vollmer receives mail at 623 W. Lincoln Ave, Oshkosh, WI, that is, the SUBJECT PREMISES. Moreover, no change of address has been filed regarding Vollmer or this address.

41. Based upon the information set forth above, there is probable cause to believe that the computer which used the IP address 69.23.82 on March 8, 2005 is located at the subject SUBJECT PREMISES along with one of its user, Samantha Vollmer.

42. Based upon my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the distribution and collection of child pornography:

a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or

other visual media; or from literature describing such activity.

b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. c.

Collectors of child pornography often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica,[4] and video tapes for many years.

d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, oftentimes at the collector's residence, to enable the collector

[4] "Child erotica," as used in this Affidavit, is defined as materials or items that are sexually arousing to certain individuals but which are not in and of themselves obscene or do not necessarily depict minors in sexually explicit poses or positions. Such material may include non-sexually explicit photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), drawings, or sketches, written descriptions/stories, or journals.

to view the collection, which is valued highly.

e. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

43. The undersigned affiant submits that there is probable cause to believe that Samantha Vollmer or an individual using her IP address 69.23.82.99 on March 8, 2005 at 14:06 CST, utilizing Time Warner-Road Runner at 623 W. Lincoln Ave., Oshkosh, WI 54901 is a collector or recipient of child pornography. This opinion is based upon (a) the child pornography images that Samantha Vollmer, or an individual associated with her computer, downloaded, that is, multiple images of both prepubescent boys and girls engaged in sexually explicit conduct; (b) that the individual downloading images from Mr. Reimann's F-serve did so from an IRC chat room with a name suggestive of child pornography; and (c)this was done so after reading Mr. Reimann's advertisement indicating his desire for uploads involving sexually explicit images of minor boys and further after observing the folder names created by Mr. Reimann that accurately summarize the content of the sexually explicit images of minors contained within.

44. Finally, based upon the conduct of individuals involved in the collection of child pornography set forth above in paragraph 37, namely, that they tend to maintain their collections at a private location for long periods of time, there is probable cause to believe that evidence of the offenses of distributing, receiving and possessing child pornography is currently located at the SUBJECT PREMISES.

Specifics Regarding the Seizure and Searching of Computer Systems

45. Based on my own experience and consultation with other agents who have been involved in the search of computers and retrieval of data from computer systems and related peripherals, and computer media, there are several reasons why a complete search and seizure of information from computers often requires seizure of all electronic storage devices, as well as all related peripherals, to permit a thorough search later by qualified computer experts in a laboratory or other controlled environment:

a. Computer storage devices, such as hard disks, diskettes, tapes, laser disks, and Bernoulli drives, can store the equivalent of hundreds of thousands of pages of information. Additionally, when an individual seeks to conceal information that may constitute criminal evidence, that individual may store the information in random order with deceptive file names. As a result, it may be necessary for law enforcement authorities performing a search to examine all the stored data to determine which particular files are evidence or instrumentalities of criminal activity. This review and sorting process can take weeks or months, depending on the volume of data stored, and would be impossible to attempt during a search on site; and

b. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even those who are computer experts to specialize in

some systems and applications. It is difficult to know before a search what type of hardware and software are present and therefore which experts will be required to analyze the subject system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis.

46. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system.

It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

c. I am familiar with and understand the implications of the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa, and the role of this statute in protecting First Amendment activities. I am not aware that any of the materials to be searched and seized from the SUBJECT

PREMISES are protected materials pursuant to the PPA. If any such protected materials are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

Conclusion

47. Based on the above information, there is probable cause to believe that 18 U.S.C. §§ 2252 and 2252A, which, among other things, make it a federal crime for any person to knowingly possess, receive, or transport child pornography, have been violated, and that the following property, evidence, fruits and instrumentalities of these offenses are located at the SUBJECT PREMISES:

a. images of child pornography and files containing images of child pornography in any form wherever it may be stored or found including, but not limited to:

i. any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation,

and any hardware/software manuals related to or used to visually depict child pornography or child erotica; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, child erotica or information pertaining to an interest in child pornography;

ii. books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

iii. originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

iv. motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

b. information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18

U.S.C. § 2256; and

ii. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

c. credit card information, including but not limited, to bills and payment records;

d. records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence; and

e. records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

This affiant requests authority to seize such material.

49. Based upon the foregoing, this affiant respectfully requests that this Court issue a search warrant for the SUBJECT PREMISES, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B.

50. It is further respectfully requested that this Court issue an Order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the

SUBJECT PREMISES). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation, and premature disclosure of the contents of this Affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness.

Special Agent, FBI

Subscribed and sworn
before me this 25th of May, 2005

HONORABLE WILLIAM C. GRIESBACH.
United States District Court Judge

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

1) A two story multi-family residence, beige in color with wood siding, white trim and dark green shingled roof. There are separate entrances with separate street addresses for each of the residences that make up this multi-family dwelling. The front door to the Subject Premises has the number "623" written above it. The rear door to the Subject Premises also has the number "623" written above it.

ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

1. Images of child pornography and files containing images of child pornography in any form wherever it may be stored or found including, but not limited to:

A. any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

B. books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

C. originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

D. motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

2. Information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

A. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

B. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

3. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence; and

4. Records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.